УДК 004.056.53
DOI: 10.31673/2409-7292.2024.040009

Толкачов М. Ю.

МЕХАНІЗМИ ЗАХИСТУ ТРАФІКУ В КІБЕРПРОСТОРІ

Предметом дослідження є інформаційні ресурсі в кіберпросторі інфокомунікаційних систем та інтернет-трафік. Доведено необхідність комплексного аналізу захисту інфокомунікаційних систем, який об'єднує кілька ключових елементів: механізми безпеки, типи та види трафіку, протоколи передачі даних і семіотичний багаторівневий підхід. Проаналізовано сучасний стан видів трафіку конвергентної мережі, структуру інфокомунікаційних систем і кібератаки на розподілені структури інфокомунікаційних систем. Розглянуто сучасний стан захисту інформаційних ресурсів, захисту типів трафіка, протоколів для різних механізмів безпеки в кіберпростірі. У цьому контексті зазначено, що конвергентна мережева інфраструктура повинна бути захищеною для передачі різноманітних інформаційних потоків, а проблема ефективного захисту інформації в умовах її зростаючих обсягів набуває критичного наукового і практичного значення. Використання семіотичної моделі дає змогу впорядкувати підходи до захисту різноманітних типів трафіку та протоколів у інфокомунікаційних мережах. Завдяки семантичному, синтаксичному та прагматичному рівням семіотичної моделі забезпечується комплексний аналіз проблем безпеки, що об’єднує технічні, структурні й соціальні аспекти. Це відіграє ключову роль у ефективному захисті розподілених мереж від сучасних загроз, які постійно ускладнюються.

Ключові слова: захист інформації, кіберпростір, інформаційні ресурси, інфокомунікаційні мережі, семіотичні принципи, механізми безпеки.

Вступ

Україна, як частина спільноти світового інформаційного суспільства, продовжує впроваджувати новітні технології, в т.ч. інформаційно-комунікаційні послуги, що сприяє розвитку економіки та суспільства, підвищує можливості реалізації людського потенціалу, використання національних ресурсів.

Із введенням 14 вересня 2020 року в дію нової Стратегії національної безпеки України було дано старт і підготовці проектів низки стратегічних документів, одним з яких є Стратегія кібербезпеки України. Стратегія кібербезпеки України (2021 – 2025 роки) визначає пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Кібербезпека є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі.

Серед основних загроз національній безпеці в інформаційній сфері чи не найголовнішим є вплив на управління передаванням інформації в розподілених інфокомунікаційних системах та мережах доставки контенту. З метою ефективного використання мережевих ресурсів глобальної інформаційної інфраструктури загалом, та її національного сегменту зокрема, шляхом підвищення продуктивності процесів передавання даних в умовах збільшення їх обсягів.

Ризик кіберзагроз є актуальним для значної кількості суб’єктів: від приватних осіб до великих компаній, окремих галузей економіки та держав загалом. На національному та міжнародному рівні наявне усвідомлення того, що проблеми кібербезпеки можуть завдати шкоди національній безпеці та дієвому функціонуванню економіки держави

Стратегія кібербезпеки України визначає пріоритети національних інтересів у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

У цій Стратегії визначено, що “забезпечення кібербезпеки є одним з пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі”.

Оцінка рівня захищеності та захист мережевого трафіку стає критично важливою задачею в епоху глобальної цифровізації. З огляду на різноманітність та обсяг наборів даних, які передаються мережами, слід зазначити, що традиційні підходи до кібербезпеки, які сфокусовані тільки на технічних аспектах захисту, виявляються недостатніми [1–4]. У міжнародних стандартах по кібербезпеці Standard ISO/IEC 27032:2023 з урахуванням тенденцій розвитку глобальної мережі Інтернет визначено поняття кіберпростору та кібербезпеки [5, 6]. Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [7].

Враховуючи динаміку розвитку інфокомунікаційних технологій та збільшення типів кіберзагроз, очевидно, що побудова високоефективного захисту інформаційної інфраструктури стає національним пріоритетом України.

Мета роботи та цілі дослідження

Метою роботи є проведення аналітичного огляду сучасних аспектів захисту інформаційних ресурсів в кіберпросторі і аналіз сучасного стану захищеності інтернет-трафіку в інфокомунікаційних системах.

Такий аналіз дозволить сформувати напрямки проектування методів безпеки інфокомунікаційних мереж, що охоплює весь стек мережної безпеки. Це дасть змогу проєктувати інформаціонну безпеку на основі застосування новітніх підходів, таких як семіотичний.

Для вирішення поставленої мети розглянуто такі завдання:

1. Проаналізувати сучасний стан кіберзагроз, механізмів захисту інформаційних ресурсів та типів інтернет-трафіку в інфокомунікаційних системах.

2. Дослідити методи забезпечення захисту від сучасних кібератак, зокрема атак на соціальний контент та розподілені інформаційні системи.

3. Визначити ключові механізми безпеки для різних протоколів передачі даних і типів трафіку з урахуванням багаторівневого семіотичного підходу (семантичного, синтаксичного та прагматичного).

4. Запропонувати підхід до моделювання та оцінки рівня захищеності різних типів трафіку з використанням семіотичної моделі.

Аналіз останніх досліджень і публікацій.

Сфери телекомунікацій та інформаційних технологій зосереджені на пошуку економічно вигідних комплексних рішень для забезпечення безпеки, які спрямовані на захист мереж від шкідливих атак та ненавмисних помилкових дій. Водночас такі рішення мають відповідати бізнес-вимогам щодо конфіденційності, цілісності та доступності інформації та послуг.

В статті [8] розглядаються підходи до моделювання поведінки агентів в інформаційно-комунікаційних системах, які є важливими для вирішення складних завдань в умовах невизначеності та змінного середовища. Проаналізовано такі методи, як агентно-орієнтоване моделювання, штучні нейронні мережі, нечітка логіка, генетичні алгоритми та ланцюги Маркова, кожен із яких має свої переваги та обмеження. Агентно-орієнтоване моделювання забезпечує гнучкість і можливість моделювати взаємодії між автономними агентами, хоча складнощі виникають при врахуванні ірраціональної поведінки. Штучні нейронні мережі дозволяють ефективно вирішувати нелінійні задачі, але вимагають великих обчислювальних ресурсів. Для підвищення ефективності пропонується адаптувати підходи до специфіки завдань і комбінувати їх для подолання існуючих обмежень.

© Толкачов, М. Ю. (2024). Механізми захисту трафіку в кіберпросторі. Сучасний захист інформації, 4(60), 85–99. https://doi.org/10.31673/2409-7292.2024.040009.

Залишаються невирішеними питання використання методів інтелектуального аналізу даних для адекватного розподілу інформації, що передається, з метою оцінки рівня захищеності [9-11], а також проблеми правильного динамічного поділу переданих даних для подальшого захисту мережі. Дані, що збираються, повинні бути представлені у зручному форматі для визначення повного та релевантного набору метрик, які відображають стан захищеності. У процесі моніторингу інформації, що передається, недостатньо враховується соціальний вплив на зміст трафіку, який може суттєво впливати на безпеку та ефективність роботи мережі. Серед доступних методів інтелектуальної обробки даних перспективним для вирішення цієї проблеми є семіотичний підхід. Він дозволяє структурувати знання про предметну область, аналізувати залежності між об’єктами, процесами та подіями, а також робити висновки щодо причинно-наслідкових зв’язків, включаючи соціальні аспекти.

У роботі [12] розглядається моделювання кіберзагроз та генерація доказових ланцюгів для критично важливих інформаційних інфраструктур. Автори акцентують увагу на необхідності захисту складних інформаційних систем від сучасних кіберзагроз, які постійно ускладнюються. Запропонована модель дозволяє створювати сценарії атак, аналізувати потенційні шляхи проникнення та розробляти докази кіберінцидентів, базуючись на виявлених подіях. Такі підходи забезпечують глибший аналіз технічних аспектів атак, розширюють знання про профілі зловмисників і сприяють поліпшенню стратегій реагування. У результаті, модель допомагає операторам критичних інформаційних інфраструктур підвищити кіберстійкість і посилити захист своїх мереж.

Робота [13] спрямована на встановлення стандартів безпеки для інформаційних систем, включаючи рекомендації щодо управління ризиками, захисту конфіденційності та контролю доступу. Основна увага приділяється систематизації засобів безпеки, методам їх впровадження та процедурам оцінки відповідності. Рекомендації з управління ризиками, викладені у NIST SP 800-53 Rev. 4, охоплюють процеси ідентифікації, оцінки, пріоритизації та реагування на ризики для забезпечення безпеки федеральних інформаційних систем.

Таким чином, на підставі проведеного аналізу, результатів вивчення наукових публікацій за темою досліджень, патентів, монографій та практичних розробок встановлено, що на сучасному етапі розвитку прогресивних інформаційних технологій остаточно не вирішено питання виявлення кіберзагроз, тому актуальним є завдання аналізу проблем безпеки, що об'єднує технічні, структурні й соціальні аспекти для виявлення складних загроз.

Проте питання безпеки інформаційних ресурсів, технологій, методів і засобів, що застосовуються для захисту інформації залишаються актуальними і потребують подальших досліджень.

Аналіз сучасного стану видів трафіку мережі та тенденції розвитку методів захисту інформаційних ресурсів.

Зі стрімким розвитком загальнодоступних мережевих технологій (зокрема, Інтернету), які відкривають значні бізнес-можливості, організації все частіше ведуть електронний бізнес у глобальному масштабі та надають онлайн-послуги населенню. Ці можливості охоплюють як недорогий обмін даними через Інтернет як глобальне середовище зв’язку, так і більш складні послуги, що надаються провайдерами інтернет-послуг (ISP). Це може включати використання відносно дешевих локальних точок підключення на кожному кінці ланцюга для повномасштабної онлайн-торгівлі та систем надання послуг, що використовують веб-додатки та сервіси.

Крім того, нові технології (зокрема інтеграція даних, голосу та відео) розширюють можливості для дистанційної роботи (також відомої як “телеробота” або “віддалена робота”) (Табл.1). Це дозволяє працівникам працювати далеко від своєї базової локації протягом тривалого часу. Вони можуть залишатися на зв’язку за допомогою віддалених засобів доступу до мереж організації та спільноти, а також до відповідної інформації та бізнес-послуг [14].

Обсяг трафіку (%) – частка цього типу трафіку у загальному обсязі інтернет-активності. Кількість користувачів (млрд) – кількість людей, що активно використовують категорію.

© Толкачов, М. Ю. (2024). Механізми захисту трафіку в кіберпросторі. Сучасний захист інформації, 4(60), 85–99. https://doi.org/10.31673/2409-7292.2024.040009.

Середній час сесії (хв.) – скільки часу в середньому витрачають користувачі за один сеанс. Загальний трафік (ТБ/день) – Оцінка трафіку у терабайтах, що генерується щоденно.

Таблиця 1

Аналіз інтернет-трафіку за категоріями та типами активності

Тип трафіку	Категорія	Обсяг трафіку (%)	Кількість користувачів (млрд)	Середній час сесії (хвилини)	Загальний трафік (ТБ/день)
Веб-серфінг	Новинні сайти	15	2.5	8	500
	Електронна комерція	20	1.8	12	650
	Освітні ресурси	10	1.2	15	300
Соціальні мережі	Facebook	30	2.9	20	900
	Instagram	15	2.1	25	600
	TikTok	15	1.5	45	550
	LinkedIn	5	0.9	10	200
Відеострімінг	YouTube	30	2.8	40	1500
	Netflix	25	1.5	120	1200
	Amazon Prime	10	0.8	90	800
Онлайн-ігри	Комп'ютерні ігри	20	1.2	60	1000
	Мобільні ігри	15	2.5	30	700
	Консольні ігри	10	0.7	120	800

Однак, хоча це середовище і забезпечує значні переваги для бізнесу, виникають нові ризики безпеки, якими потрібно керувати. Оскільки організації значною мірою залежать від використання інформації та пов’язаних із нею мереж для ведення своєї діяльності, втрата конфіденційності, цілісності та доступності інформації та послуг може мати значні негативні наслідки для бізнес-операцій. Таким чином, існує важлива потреба у належному захисті мереж, пов’язаних із ними інформаційних систем та даних. Іншими словами: впровадження та підтримка адекватної мережевої безпеки є абсолютно необхідними для успішного функціонування бізнес-операцій будь-якої організації.

У контексті галузей телекомунікацій та інформаційних технологій важливо знаходити економічно вигідні комплексні рішення з безпеки, які спрямовані на захист мереж від шкідливих атак і ненавмисних помилкових дій, а також на забезпечення бізнес-вимог щодо конфіденційності, цілісності та доступності інформації та послуг. Захист мережі також має вирішальне значення для підтримання точності даних про оплату або використання залежно від обставин. Можливості безпеки у продуктах є критично важливими для загальної безпеки мережі (включно з додатками та послугами). Проте зі збільшенням кількості продуктів, об’єднаних для створення комплексних рішень, сумісність або її відсутність визначатимуть успішність рішення. Безпека має бути не лише складовою кожного продукту чи послуги, а й розроблятися таким чином, щоб забезпечувати взаємозв’язок можливостей безпеки у загальному рішенні з безпеки.

Сучасне суспільство активно застосовує різні форми соціальної та економічної діяльності, що ґрунтуються на широкому використанні інформаційних і телекомунікаційних технологій. Науково-технічний прогрес сприяє переходу від постіндустріального до інформаційного суспільства. Водночас удосконалюються методи хакерів, які використовують штучний інтелект, соціальну інженерію та експлойти нульового дня. Виходячи з принципів і положень державної політики забезпечення інформаційної безпеки, найбільшу загрозу становлять ризики для інформаційних ресурсів у політичній, економічній, оборонній та інших сферах діяльності держави (Табл. 2). Під загрозою у широкому сенсі зазвичай розуміють потенційно можливу подію, дію (вплив), процес або явище, які можуть призвести до завдання шкоди будь-якій зі сторін. У табл. 3 наведено загальну класифікацію загроз інформаційним ресурсам.

Таблиця 2

Інформаційні ресурси в різних сферах діяльності держави

Сфера діяльності	Інформаційні ресурси
Оборонна сфера	Центральний апарат МО, ГШ, головні штаби видів ЗСУ і родів військ
	Пункти управління системи управління військами і зброєю, їхнє інформаційне забезпечення
	Інформаційні ресурси науково-дослідних установ МО
	Інформаційні ресурси підприємств оборонного комплексу
	Центри обробки та аналізу інформації ГШ і підрозділів штабів видів ЗСУ, об’єднань і з’єднань видів і родів ЗСУ
	Вузли та лінії радіозв’язку, радіорелейного, тропосферного і супутникового зв’язку, а також лінії проводового зв'язку, відомчі та орендовані МО і іншими силовими структурами
	Системи зв’язку та управління військами і зброєю, їхнє інформаційне забезпечення
Політична сфера	Система прийняття політичних рішень
	Система формування громадської думки
	Система інформування населення органами державної влади
	Система інформаційно-пропагандистського впливу
Сфера економіки	Система державної статистики
	Джерела інформації про комерційну діяльність, споживчі властивості товарів і послуг
	Системи збору та обробки фінансової, біржової, податкової, митної інформації
	Системи збору та обробки інформації про зовнішньоекономічну діяльність держави і комерційних структур
	Система соціально-політичної і економічної орієнтації

Таблиця 3

Основні загрози безпеці інформації

Категорія загроз	Підкатегорія	Тип дії	Приклади ситуацій	Можливі наслідки
Штучні	Навмисні	Зловмисні дії	- Несанкціонований доступ (злом) - Впровадження вірусів - Використання апаратних чи програмних закладок	- Втрата конфіденційної інформації - Порушення роботи систем
		Шахрайство	- Маскування під легітимного користувача - Використання фішингових сайтів	- Викрадення персональних даних - Фінансові втрати
	Ненавмисні	Помилки персоналу	- Неправильне налаштування систем - Несанкціоноване розкриття даних	- Витік інформації - Порушення конфіденційності
		Програмні помилки	- Вади в алгоритмах роботи програмного забезпечення - Неправильне оновлення систем	- Втрата даних - Збої в роботі системи
Природні		Стихійні явища	- Землетруси, повені, пожежі	- Руйнування апаратного забезпечення - Переривання роботи
		Зовнішні фактори старіння	- Зношення кабелів - Старіння апаратного забезпечення	- Падіння продуктивності - Втрата доступу до ресурсів

Основними напрямами державної політики у сфері забезпечення безпеки національних інформаційних ресурсів є застосування комплексних заходів щодо їх захисту, розробка і впровадження необхідних засобів і режимів отримання, зберігання, поширення та використання інформації, створення розвинутої інфраструктури в інформаційній сфері, а

© Толкачов, М. Ю. (2024). Механізми захисту трафіку в кіберпросторі. Сучасний захист інформації, 4(60), 85–99. https://doi.org/10.31673/2409-7292.2024.040009.

також розробка і впровадження сучасних технологій та засобів захисту інформації. Кіберпростір, поряд з іншими фізичними просторами, визнаний одним із можливих театрів воєнних дій. Тому здатність держави захищати національні інтереси в ньому є ключовим елементом забезпечення кібербезпеки.

Сучасний стан і тенденції розвитку методів захисту інформаційних ресурсів у кіберпросторі зумовлені стрімкою цифровізацією, складністю кіберзагроз та необхідністю захисту даних в умовах постійної взаємодії між різними системами. Основні виклики у сфері захисту інформаційних ресурсів включають зростання кількості кіберзагроз, таких як фішинг, програми-вимагачі (ransomware), APT (Advanced Persistent Threat), DDoS-атаки, а також ускладнення інфраструктури через впровадження хмарних технологій, Інтернету речей (IoT) і розподілених систем. Додаткові проблеми становить людський фактор, зокрема помилки співробітників і ненавмисне розкриття даних, а також необхідність відповідності регуляторним вимогам, таким як GDPR, ISO 27001 та інші.

Сучасний стан захисту інформаційних ресурсів характеризується використанням багатофакторної аутентифікації (MFA), яка поєднує паролі, біометричні дані та одноразові паролі (OTP), активним застосуванням криптографічних методів (AES, RSA) для шифрування даних під час зберігання та передачі, впровадженням систем виявлення вторгнень (IDS) і запобігання (IPS) для автоматизованого аналізу трафіку, захистом даних у хмарних середовищах завдяки Cloud Access Security Broker (CASB) та використанням аналітики великих даних для виявлення аномалій і прогнозування загроз [15–21].

Масштаби викликів та необхідність у сучасних методах захисту інформаційних ресурсів визначають тенденції розвитку методів захисту інформаційних ресурсів (Табл. 4). Тенденції розвитку включають інтеграцію штучного інтелекту (AI) та машинного навчання (ML) для виявлення аномалій, автоматизації реагування на інциденти та прогнозування загроз.

Таблиця 4

Статистика сучасних кіберзагроз, факторів ризику та їх впливу

Категорія	Приклад	Статистика	Джерело/Рік
Кіберзагрози	Фішинг	36% усіх атак у світі пов’язані з фішингом	Verizon DBIR, 2023
	DDoS-атаки	15 млн атак було зафіксовано у 2022 році	NETSCOUT Threat Report, 2023
	Програми-здирники	Збитки від атак досягли $20 млрд у 2022 році	Cybersecurity Ventures, 2023
Складність інфраструктури	Хмарні сервіси	60% компаній зберігають критичні дані в хмарі	Flexera State of Cloud Report, 2023
	Інтернет речей (IoT)	25 млрд підключених пристроїв IoT очікується до 2030 року	Statista, 2023
Людський фактор	Помилки співробітників	82% інцидентів кібербезпеки спричинені людським фактором	IBM Cost of Data Breach Report, 2023
	Ненавмисне розкриття даних	Середній збиток від однієї витоку даних — $4,45 млн	IBM Cost of Data Breach Report, 2023
Регуляторні вимоги	GDPR	1,5 млрд євро штрафів накладено з моменту впровадження GDPR	CMS GDPR Enforcement Tracker, 2023
	ISO 27001	39% організацій мають сертифікацію ISO 27001 для відповідності стандартам	Deloitte Global Survey, 2023

Спостерігається розвиток постквантової криптографії для захисту від потенційних загроз квантових комп’ютерів. Постквантова криптографія (Post-Quantum Cryptography) створюється вже зараз, щоб протистояти загрозам, які з’являться з розвитком квантових комп’ютерів. Крім того, конфіденційні обчислення (Confidential Computing) дозволяють

© Толкачов, М. Ю. (2024). Механізми захисту трафіку в кіберпросторі. Сучасний захист інформації, 4(60), 85–99. https://doi.org/10.31673/2409-7292.2024.040009.

шифрувати дані навіть під час їхньої обробки, що є надзвичайно корисним для компаній, які працюють із чутливою інформацією, наприклад, медичними даними.

Таблиця 5

Статистика щодо сучасних кіберзагроз, факторів ризику та їх впливу

Категорія	Приклад	Статистика	Джерело/Рік
Кіберзагрози	Фішинг	36% усіх атак у світі пов'язані з фішингом	Verizon DBIR, 2023
	DDoS-атаки	15 млн атак було зафіксовано у 2022 році	NETSCOUT Threat Report, 2023
	Програми-здирники	Збитки від атак досягли $20 млрд у 2022 році	Cybersecurity Ventures, 2023
Складність інфраструктури	Хмарні сервіси	60% компаній зберігають критичні дані в хмарі	Flexera State of Cloud Report, 2023
	Інтернет речей (IoT)	25 млрд підключених пристроїв IoT очікується до 2030 року	Statista, 2023
Людський фактор	Помилки співробітників	82% інцидентів кібербезпеки спричинені людським фактором	IBM Cost of Data Breach Report, 2023
	Ненавмисне розкриття даних	Середній збиток від однієї витоку даних — $4,45 млн	IBM Cost of Data Breach Report, 2023
Регуляторні вимоги	GDPR	1,5 млрд євро штрафів накладено з моменту впровадження GDPR	CMS GDPR Enforcement Tracker, 2023
	ISO 27001	39% організацій мають сертифікацію ISO 27001 для відповідності стандартам	Deloitte Global Survey, 2023

Ще одна цікава тенденція – захист пристроїв Інтернету речей (IoT). Наприклад, розумний дім, у якому лампи, камери й термостати підключені до Інтернету. Якщо зловмисники отримають доступ до одного пристрою, вони можуть атакувати всю систему. Щоб уникнути цього, розробляються легкі протоколи шифрування і сегментований підхід до мережевої безпеки IoT, коли кожен пристрій має окремий рівень захисту. Використання блокчейну для забезпечення незмінності даних, безпеки транзакцій та управління доступом.

Впровадження архітектури Zero Trust Architecture (ZTA), яка передбачає перевірку кожного запиту незалежно від його джерела чи розташування по принципу "не довіряй, перевіряй", створення систем протидії соціальній інженерії, включаючи аналіз фішингових повідомлень та навчання працівників, а також інтеграцію безпеки на всіх етапах розробки програмного забезпечення через підходи DevSecOps.

Перспективи розвитку методів захисту інформаційних ресурсів включають розвиток конфіденційних обчислень (Confidential Computing), де дані залишаються зашифрованими навіть під час обробки, розширення використання біометричних методів ідентифікації, вдосконалення захисту в реальному часі за допомогою AI, а також інтеграцію захисту в усі компоненти цифрової інфраструктури, включаючи хмарні та гібридні середовища.

Кібератаки як джерело загроз на різні типи трафіку інфокомунікаційних систем

Термін "інфокомунікації" описує нерозривний зв'язок між інформаційними та телекомунікаційними компонентами інформаційного обміну, які розвиваються в результаті конвергенції [22]. Поєднання цих технологій спричинило реорганізацію мережевої архітектури та створення інфокомунікаційних мереж нового покоління (Next Generation Networks, NGN), що надають мультисервісні послуги з постійним зростанням інтенсивності мережевого трафіку. Впровадження нових інформаційно-комунікаційних сервісів, перенесення традиційних послуг на платформу IP, а також збільшення кількості користувачів цих сервісів стимулювали розвиток технологій, де ключовим є забезпечення безпеки доставки послуг кінцевим споживачам. Особливої актуальності ці питання набувають у зв'язку з

© Толкачов, М. Ю. (2024). Механізми захисту трафіку в кіберпросторі. Сучасний захист інформації, 4(60), 85–99. https://doi.org/10.31673/2409-7292.2024.040009.

необхідністю забезпечення високої продуктивності мережевої інфраструктури та ефективного використання мережевих ресурсів для передачі зростаючих обсягів трафіку. Ці тенденції підвищують вимоги до управління трафіком у телекомунікаційних системах. Для задоволення цих вимог у системах передачі даних впроваджуються методи й механізми захисту трафіку, які певною мірою враховують специфіку різних видів протоколів і послуг. Зростання нових типів загроз, таких як соціокіберсистемні атаки, цільові кібератаки та внутрішні порушення, підвищує вимоги до інформаційних мереж, які стають основою забезпечення якісного захисту інформації.

Існуючі підходи до поділу інформаційних потоків, наприклад, із використанням статичного одноетапного тегування в Zero Trust Security [23], виявляються недостатніми для подальшого аналізу та захисту інформаційних систем, що підтверджується зафіксованими випадками успішних кібератак. До того ж, такі підходи не враховують особливостей відносно нових типів інформаційних систем, як-от Інтернет речей, промисловий Інтернет речей, соціальні мережі та оброблювані ними дані. У результаті з'являються нові підходи до забезпечення захисту інформаційних систем, зокрема ті, що базуються на постійному динамічному моніторингу поведінки інформаційної системи.

Сучасні інфокомунікаційні системи з розподіленою структурою стають дедалі складнішими та вразливішими до кіберзагроз. Оскільки ці системи обробляють різноманітні види трафіку, наприклад, реального часу, потоковий, еластичний, сигнальний, виникає потреба в захисті кожного з них від цільових кібератак. Основні моделі кібератак враховують тип трафіку та особливості розподіленої структури інфокомунікаційних систем. Для того щоб розуміти, як і на яких рівнях можуть бути здійснені атаки на різні види трафіку, важливо враховувати їхні специфічні характеристики та використовувані протоколи (Табл. 6).

Трафік реального часу. Трафік реального часу включає IP-телефонію, відеоконференції та онлайн-ігри. Цей тип трафіку дуже чутливий до затримок, джитера (коливань затримки) і втрат даних. Протоколи, які часто використовуються для передачі такого трафіку, – RTCP, RSVP, UDP, і RTP. Атаки на цей трафік можуть бути спрямовані на затримку або спотворення пакетів даних, що призводить до погіршення якості зв'язку або його переривання. Часто використовуються атаки типу "відмова в обслуговуванні" (DoS), які можуть паралізувати передачу даних реального часу.

Потоковий трафік. До потокового трафіку належать аудіо та відео на вимогу (наприклад, стрімінгові сервіси), а також інтернет-радіо. Для такого трафіку характерна менша чутливість до затримок порівняно з реальним часом, але є чутливість до джитера і втрат. Потоковий трафік зазвичай передається протоколами RSVP, UDP, TCP і SCTP. Атаки на цей вид трафіку можуть зменшити якість послуг, призводити до переривання трансляції або уповільнення передачі. Використання DoS-атак на потоковий трафік може викликати істотне навантаження на сервери, що обслуговують мультимедійний контент.

Еластичний трафік. Еластичний трафік включає передачу документів, анімацію, передачу файлів, електронну пошту. Його особливістю є висока чутливість до втрат і коливань затримки, тому що часто потрібна повна передача даних. Основний протокол для еластичного трафіку – TCP, який забезпечує надійну доставку даних. Атаки на еластичний трафік можуть включати викрадення даних, MITM (атаки типу "людина посередині"), фішинг та інші види втручання, спрямовані на доступ до конфіденційної інформації або порушення її цілісності.

Сигнальний трафік. Сигнальний трафік використовується для ініціалізації сеансів зв'язку, а також для взаємодії мережевих пристроїв. Він має низьку чутливість до затримок, але високу чутливість до втрат, оскільки сигналізація є критичною для підтримки стабільного зв'язку в мережі. До протоколів для цього виду трафіку належать SIP, H.232, MGCP, H.248. Атаки на сигнальний трафік можуть включати спуфінг (підробку) сигналів, перехоплення сесій та відмову в обслуговуванні, що може спричинити повну втрату зв'язку між пристроями в мережі.

© Толкачов, М. Ю. (2024). Механізми захисту трафіку в кіберпросторі. Сучасний захист інформації, 4(60), 85–99. https://doi.org/10.31673/2409-7292.2024.040009.

Таблиця 6

Типи кібератак з урахуванням видів трафіку в інфокомунікаційних системах

Типи атак	Мета атаки	Об'єкт атаки	Тип трафіку	Протоколи (Рівень OSI)	Суб'єкт атаки
Порушення доступності	Отримання доступу до системи, виконання атак типу DDoS	Сервери, локальні мережі, додатки	Реального часу	Мережевий: IPv4, IPv6, ICMP Транспортний: UDP	Користувачі, зовнішні хости
Порушення конфіденційності	Сканування мереж, перехоплення даних (сніфінг), фішинг	Файли, бази даних, інформаційні сховища	Потоковий	Канальний: Ethernet Мережевий: ARP, IP Транспортний: TCP, SCTP	Хакери, внутрішні сегменти
Порушення цілісності	Модифікація даних, внесення змін до IP, підміна DNS	Фінансові системи, телекомунікації	Еластичний	Прикладний: DNS, HTTPS Мережевий: IP Транспортний: TCP	Внутрішні користувачі, зовнішні пристрої
Блокування систем захисту	Знищення або виведення з ладу захисного обладнання, поширення шкідливого ПЗ	Засоби управління, міжмережеві екрани, маршрутизатори	Сигналізаційний	Мережевий: ICMP Прикладний: SNMP, SIP, H.323	Зовнішні мережеві актори, зловмисні боти
Соціальна інженерія	Збір інформації через обман, маніпуляції, розсилання фішингових повідомлень	Користувачі, паролі, персональні дані	Усі типи	Прикладний: SMTP, POP3, IMAP, HTTP	Зовнішні соціальні фактори, внутрішні зловмисники
Використання вразливостей	Застосування експлойтів, SQL-ін'єкції, кібершпигунство	Веб-додатки, хмарні системи	Реального часу, еластичний	Прикладний: HTTP, SQL Мережевий: IP Транспортний: TCP	Кіберзлочинці, міжнародні групи

Захист різних типів трафіку в інфокомунікаційних системах нерозривно пов'язаний із забезпеченням стабільного функціонування інформаційної інфраструктури, яка слугує базисом для всіх процесів обробки, збереження та передачі даних. Інформаційна інфраструктура об'єднує електронні інформаційні ресурси, автоматизовані системи, засоби зв'язку та інституційні компоненти, формуючи цілісну екосистему, яка підтримує життєздатність сучасних інформаційно-комунікаційних технологій. Саме інтеграція цих елементів дозволяє забезпечити як управління різноманітними потоками даних, так і їх захист від потенційних кіберзагроз.

Оскільки сервіси та протоколи займають важливе місце в архітектурі глобальної інформаційної інфраструктури (ГІІ), стає можливим адаптувати властивості мережевої інфраструктури до потреб інфокомунікаційних послуг. У загальному випадку їх можна розділити на дві категорії: основні та додаткові (Рис. 1).

На рисунку 1 представлено взаємозв'язок між властивостями мережевої інфраструктури, типами трафіку, протоколами та механізмами безпеки, що забезпечують ефективність та надійність інформаційно-комунікаційних систем. Основні властивості, такі як мобільність, якість, надійність, продуктивність, керованість і безпека, визначають ключові вимоги до функціонування мережі. До додаткових властивостей відносяться можливість взаємодії, мінімальність вимог, доступність, масштабованість, прийнятність вартості та підтримка

національних особливостей, які розширюють можливості мережевої інфраструктури. Ці властивості безпосередньо впливають на типи трафіку, які поділяються на реального часу, потоковий, еластичний і сигнальний. Кожен тип трафіку підтримується певними протоколами, наприклад, RTP та RSVP для трафіку реального часу або TCP та HTTP для еластичного трафіку. У свою чергу, кожен тип трафіку захищений відповідними механізмами безпеки, такими як шифрування трафіку, контроль доступу до мережі чи захист від атак типу “людина посередині”. Для трафіку реального часу застосовуються механізми шифрування аудіо- і відеоданих, у той час як для сигнального трафіку використовуються механізми аутентифікації та моніторингу активності. Потоковий трафік захищений обмеженням доступу через DRM та фільтрацією трафіку, а для еластичного трафіку застосовуються антивірусні системи та сканери вразливостей.

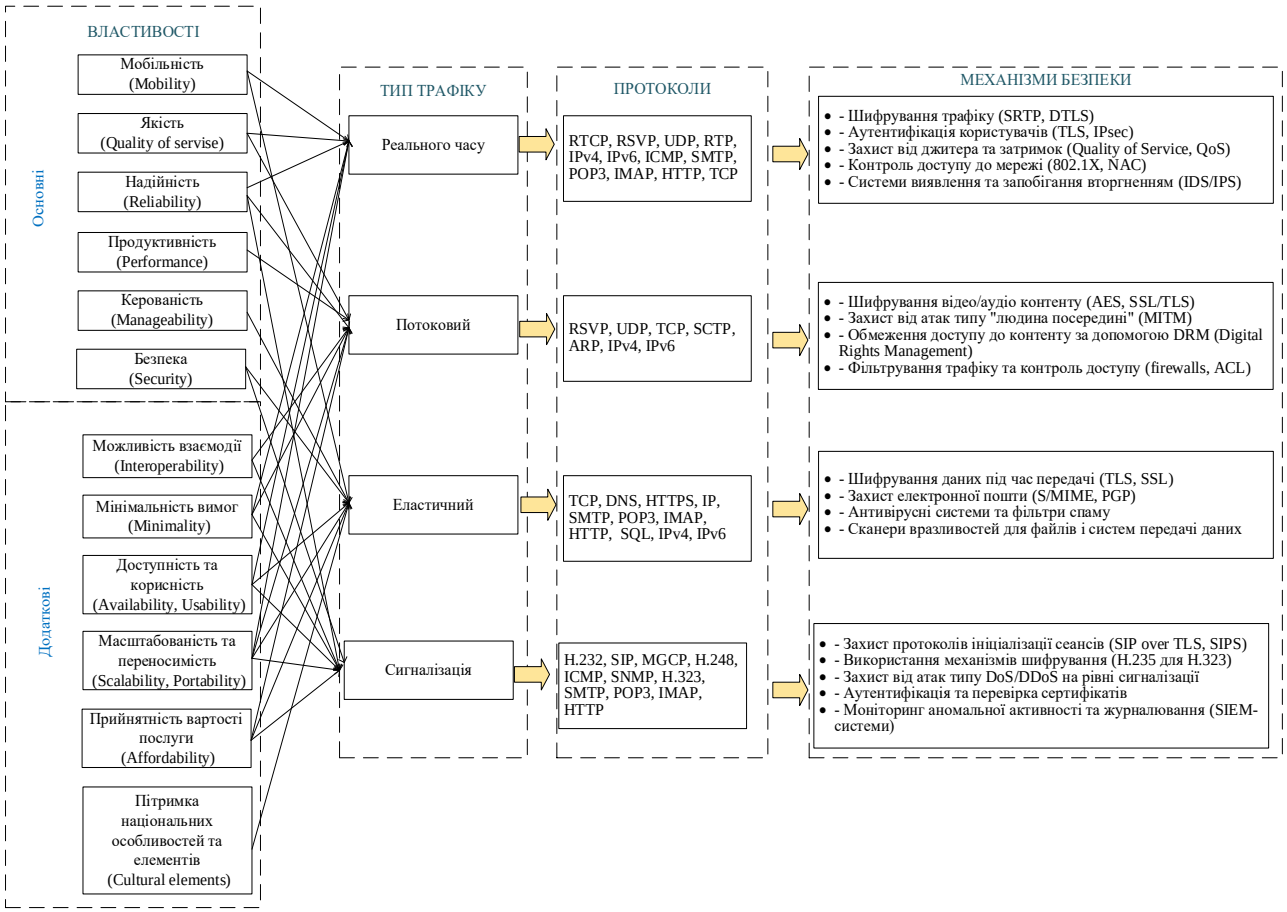

Рис. 1. Взаємозв’язок між властивостями мережевої інфраструктури, типами трафіку, протоколами та механізмами безпеки

Основні відмінності інфокомунікаційних послуг і протоколів від традиційних представлено на рис. 2.

Інфокомунікаційні послуги здебільшого є мультимедійними, що забезпечує їхню інтерактивність і багатофункціональність. Вони характеризуються широкосмуговим доступом і підтримують специфічні протоколи рівнів надання послуг моделі OSI, що дозволяє трансформувати та зберігати інформацію для подальшого використання в будь-якому часовому масштабі, включаючи реальний час. Основними відмінностями інфокомунікаційних послуг від традиційних є їх мультимедійність, широкосмуговість, використання специфічних протоколів для забезпечення різних рівнів моделі OSI та управління послугами, додаткова адресація для ідентифікації споживачів, а також клієнт-серверна підтримка їх функціонування.

© Толкачов, М. Ю. (2024). Механізми захисту трафіку в кіберпросторі. Сучасний захист інформації, 4(60), 85–99. https://doi.org/10.31673/2409-7292.2024.040009.

Клієнтська частина забезпечується програмно-апаратною платформою користувача, а серверна – платформою постачальника послуг. Важливою особливістю цих послуг є їхній інформаційний характер, оскільки дані, які складають зміст послуг, можуть бути збережені, оброблені й надані користувачам у будь-який зручний час.

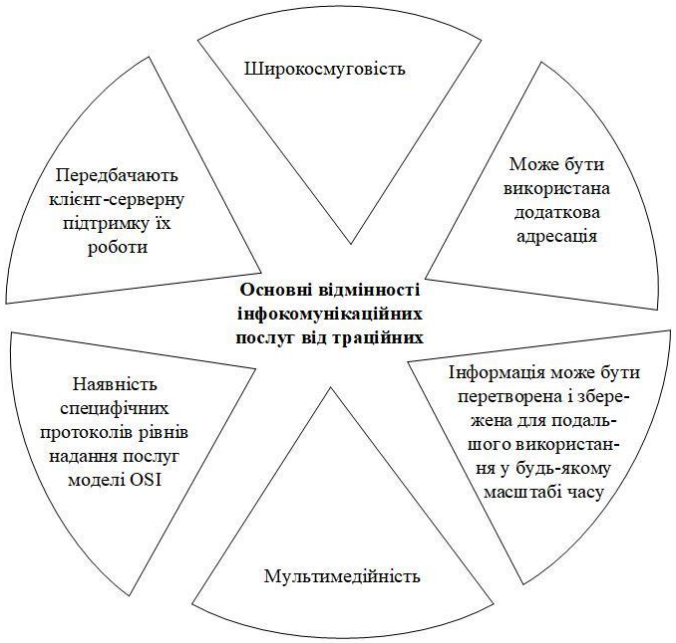

Рис. 2. Основні відмінності інфокомунікаційних послуг і протоколів

Розподілені системи мають низку переваг у порівнянні з централізованими, що робить їх особливо актуальними в сучасному кіберпросторі. Вони забезпечують можливість паралельного виконання обчислень, дозволяють досягати високої загальної продуктивності, сприяють більш ефективному спільному використанню ресурсів і пропонують оптимальне співвідношення ціни та якості. Крім того, такі системи характеризуються високою надійністю і відмовостійкістю, що є критично важливим у світі, де кіберзагрози стають дедалі складнішими.

Проте в контексті розподілених систем виникають нові виклики для кібербезпеки. На відміну від централізованих систем, розподілені мають більшу кількість вузлів, які можуть стати потенційними точками атаки. Такі загрози, як компрометація окремих компонентів, маніпуляції з переданими даними та несанкціонований доступ до ресурсів, значно ускладнюють побудову захисних механізмів. Розподілений характер цих систем також створює додаткові труднощі у забезпеченні цілісності даних, аутентифікації та контролю доступу.

Таким чином, хоча розподілені системи мають значні переваги в продуктивності, ефективності використання ресурсів і стійкості до збоїв, вони також ставлять перед кібербезпекою нові завдання. Ефективний захист таких систем потребує комплексного підходу, що враховує їх специфіку, а також сучасні загрози, характерні для кіберпростору.

Аналіз захисту інфокомунікаційних систем

Мережеві технології сьогодні є однією з найпрогресивніших галузей науки і техніки. Однак зростаюча складність інфраструктури, поява нових видів атак і недостатня ефективність існуючих алгоритмів вимагають принципово нових підходів до забезпечення інформаційної безпеки. Традиційні моделі аналізу трафіку та методи розподілу мережевих ресурсів не відповідають рівню сучасного технічного прогресу, що значно ускладнює захист інформаційно-комунікаційних технологій. Особливо це стосується гетерогенних

© Толкачов, М. Ю. (2024). Механізми захисту трафіку в кіберпросторі. Сучасний захист інформації, 4(60), 85–99. https://doi.org/10.31673/2409-7292.2024.040009.

інфокомунікаційних мереж, які передають контент різноманітного характеру – від відео- та аудіопотоків до великих обсягів службових даних.

Щоб зрозуміти, як ефективно забезпечувати безпеку гетерогенних інфокомунікаційних мереж, важливо звернути увагу на аналіз рівня захищеності протоколів за різними механізмами безпеки. У цьому контексті особливу роль відіграють такі механізми, як шифрування, автентифікація, контроль доступу та цілісності даних, нотаризація та соціальна взаємодія. Діаграма (рис. 3) нижче ілюструє, як ці механізми впливають на рівень безпеки протоколів, демонструючи різницю у відсотковому захисті залежно від застосованих засобів.

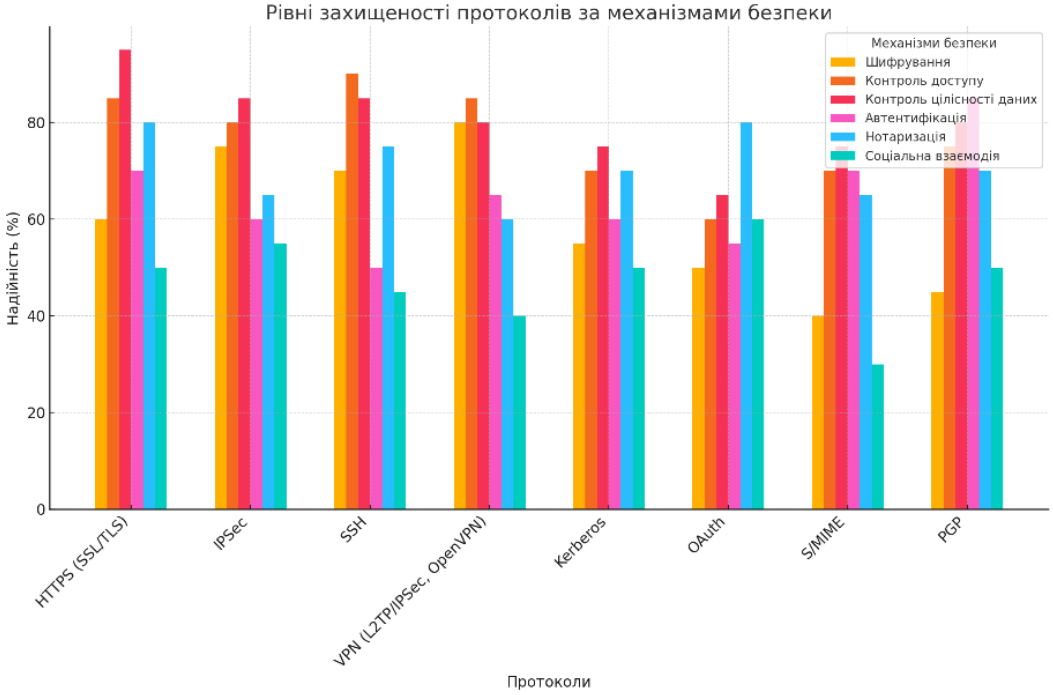

Рис. 3. Рівні захищеності протоколів за механізмами безпеки.

Таким чином, конвергентна мережева інфраструктура повинна бути захищеною для передачі різноманітних інформаційних потоків, а проблема ефективного захисту інформації в умовах її зростаючих обсягів набуває критичного наукового і практичного значення. Це вимагає розроблення нових моделей і методів доставки контенту, які враховують сучасні загрози та особливості мережевих середовищ.

У цьому контексті важливо не лише забезпечити захист даних, але й розуміти їхній зміст, адже саме значення переданої інформації може відігравати ключову роль у визначенні пріоритетів кіберзахисту. Для цього доцільно застосовувати підходи, які базуються на інтелектуальному управлінні даними, що дозволяють уточнювати та розшифровувати зміст інформації. Тут особливу роль відіграє семіотика – наука про значення, яка стає основою для розуміння понять інформації, смислу, пізнання та комунікації.

Застосування семіотичних принципів дозволяє не лише формувати змістовно пов’язані моделі кіберзахисту, але й адаптувати їх до конкретних контекстів і завдань. Поділ загальної моделі на рівні семіотики дає змогу побудувати гнучкі системи захисту, які враховують як технічні характеристики трафіку, так і змістовну складову даних, забезпечуючи тим самим максимально ефективну адаптацію до сучасних кіберзагроз.

Однак для досягнення цієї мети необхідний комплексний аналіз захисту інфокомунікаційних систем, який об’єднує кілька ключових елементів: механізми безпеки, типи та види трафіку, протоколи передачі даних і семіотичний багаторівневий підхід. Такий підхід дозволяє поєднати технічну складову захисту із семантичною, створюючи універсальні

© Толкачов, М. Ю. (2024). Механізми захисту трафіку в кіберпросторі. Сучасний захист інформації, 4(60), 85–99. https://doi.org/10.31673/2409-7292.2024.040009.

моделі безпеки, що одночасно враховують фізичні параметри мережі, контент переданих даних і їхнє значення для користувачів.

Використовуючи парадигму семіотики та перетворення розділеної інформації за допомогою динамічних наборів уявлень можна оцінити рівні захищеності механізмів безпеки на різних рівнях семіотичної моделі [10].

Рисунок 4 демонструє загальні відсоткові показники надійності кожного механізму безпеки на основі типових статистичних даних з кібербезпеки. Це базується на доступних звітах, які аналізують ефективність різних механізмів [15-21].

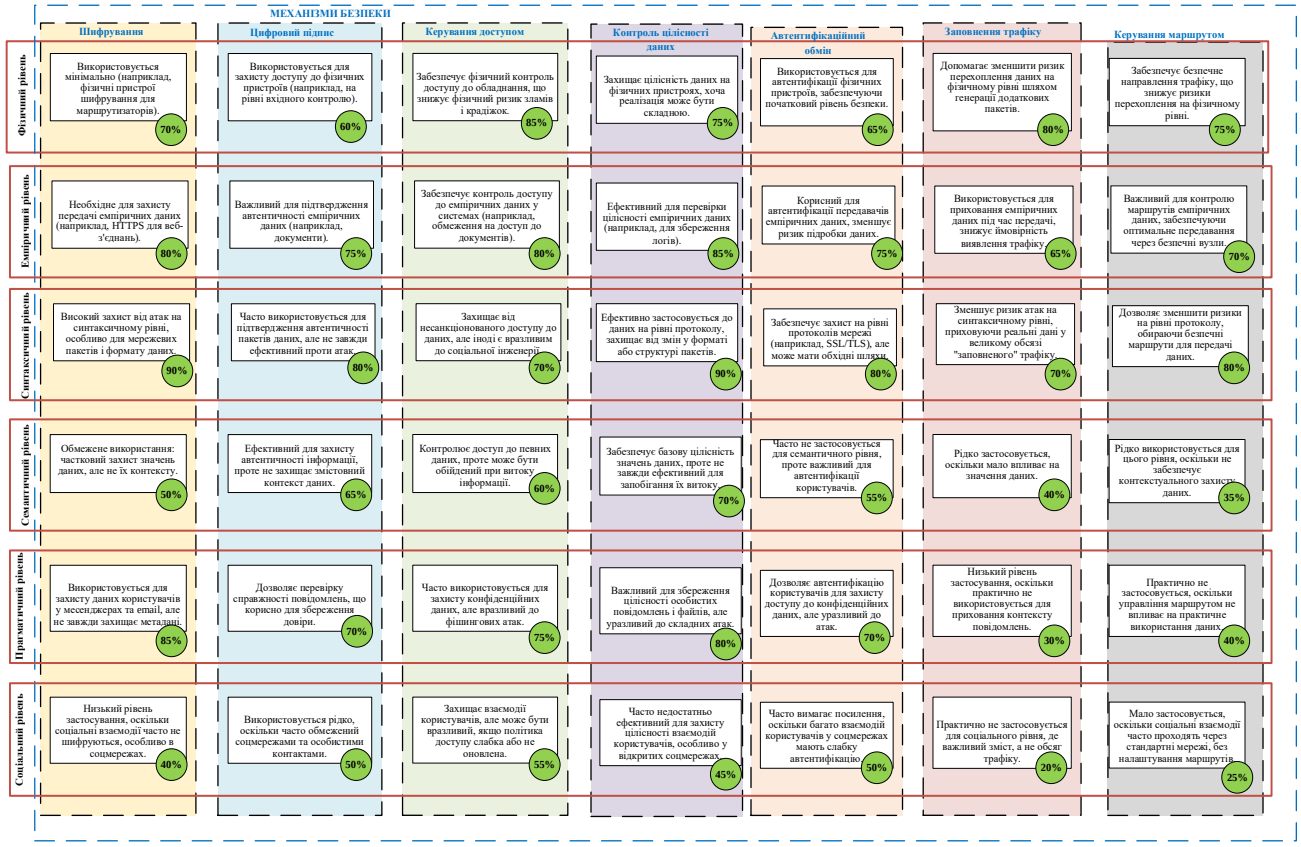

Рис 4. Надійність механізмів безпеки за рівнями (у відсотках)

Проведений аналіз підтверджує важливість використання семіотичної моделі як ефективного інструменту для захисту розподілених інфокомунікаційних систем від складних атак, що включають соціальний контент. У таблиці представлені рівні захисту різних протоколів за ключовими механізмами безпеки, такими як шифрування, контроль доступу, контроль цілісності даних, автентифікація, нотаризація та соціальна взаємодія. Дані таблиці демонструють варіативність рівнів захисту, що залежить від використаних механізмів і типів трафіку.

На семантичному рівні було виявлено, що протоколи з сильним шифруванням, наприклад, HTTPS/SSL та SSH, забезпечують найвищий рівень захисту від перехоплення і модифікації даних. Їхня ефективність у розподілених системах є особливо важливою для передачі соціального контенту, який може бути цінним об’єктом для фішингових атак або маніпуляцій. Сильні механізми контролю доступу та автентифікації, реалізовані в протоколах, таких як IPsec або Kerberos, гарантують збереження приватності інформації та запобігають несанкціонованому доступу, що є критичним для захисту чутливих даних у великих розподілених мережах.

На синтаксичному рівні доведено, що протоколи, орієнтовані на забезпечення цілісності даних, такі як OpenVPN та IPsec, мають високі показники захисту від атак типу SQL-ін’єкцій

чи маніпуляцій форматами передачі даних. Водночас використання менш захищених протоколів, наприклад, PGP, демонструє, що недостатня увага до контролю структури даних може значно знижувати стійкість до кіберзагроз.

Прагматичний рівень, що враховує специфіку використання соціального контенту, показує важливість механізмів нотаризації та соціальної взаємодії для протидії складним сценаріям атак. Протоколи, які включають ці механізми, зокрема Kerberos, забезпечують захист від атак соціальної інженерії, зловживань довірою користувачів або дестабілізації комунікацій. Такі механізми є особливо важливими для розподілених систем, у яких соціальний трафік має високу інтенсивність.

Таким чином, підтверджується, що застосування семіотичної моделі дозволяє систематизувати підходи до захисту різних типів трафіку та протоколів в інфокомунікаційних мережах. Семантичний, синтаксичний і прагматичний рівні сприяють комплексному вирішенню проблеми безпеки, поєднуючи технічні, структурні й соціальні аспекти. Це є ключовим фактором для ефективного захисту розподілених мереж від сучасних загроз, що постійно ускладнюються.

Висновки

У статті виконано аналіз сучасного стану кіберзагроз, механізмів захисту інформаційних ресурсів і типів інтернет-трафіку в інфокомунікаційних системах. Встановлено, що зі зростанням обсягів переданої інформації та кількості кібератак ефективність традиційних методів захисту суттєво знижується. Виявлено, що конвергентна мережева інфраструктура, яка забезпечує передачу різноманітних інформаційних потоків, потребує інтеграції багаторівневих механізмів захисту. Особливу увагу приділено аналізу впливу атак на соціальний контент та розподілені інформаційні системи, що вимагає розробки нових підходів до безпеки.

Дослідження методів захисту від сучасних кібератак підтвердило необхідність урахування специфіки різних видів трафіку. Визначено, що такі загрози, як фішинг, атаки типу DDoS, програми-вимагачі та маніпуляції з соціальним контентом, мають значний вплив на інформаційні системи. Для протидії цим загрозам рекомендовано використовувати сучасні технології, зокрема штучний інтелект, машинне навчання та постквантову криптографію, які забезпечують динамічний моніторинг та адаптацію до нових ризиків.

Запропоновано багаторівневий підхід до визначення механізмів безпеки для різних протоколів передачі даних і типів трафіку. Семіотична модель, яка враховує семантичний, синтаксичний та прагматичний рівні, дозволяє здійснити комплексний аналіз захищеності інформації. На семантичному рівні забезпечується шифрування та автентифікація, на синтаксичному – контроль цілісності даних, а на прагматичному – захист соціального контенту від атак соціальної інженерії.

Також запропоновано підхід до моделювання та оцінки рівня захищеності різних типів трафіку з використанням семіотичної моделі. Цей підхід забезпечує систематизацію методів безпеки відповідно до специфіки трафіку та протоколів, дозволяючи створювати ефективні стратегії захисту. Завдяки семантичному, синтаксичному та прагматичному рівням семіотичної моделі можна здійснити комплексний аналіз безпеки, який об’єднує технічні, структурні та соціальні аспекти. Це дозволяє створити ефективні стратегії захисту для розподілених інфокомунікаційних мереж, здатних протистояти сучасним кіберзагрозам, які постійно еволюціонують і ускладнюються.

Перелік посилань

1. Broadband Search: “Key Internet Statistics in 2023 (Including Mobile)”. https://datareportal.com/reports/digital-2023-global-overview-report

2. A Method of Protecting Information in Cyberphysical Space / N. Dzheniuk, S. Yevseiev, B. Lazurenko, O. Serkov, O. Kasilov // Advanced Information Systems. – 2023. – Volume 7, Number 4. – P. 80-85 **doi:** https://doi.org/10.20998/2522-9052.2023.4.11

© Толкачов, М. Ю. (2024). Механізми захисту трафіку в кіберпросторі. Сучасний захист інформації, 4(60), 85–99. https://doi.org/10.31673/2409-7292.2024.040009.

3. Спосіб генерації широкосмугового імпульсного сигналу та антена для його реалізації / Серков О.А., Бреславець В.С. Перова І.Г. Толкачов М.Ю. Чурюмов Г.І. // Патент України на винахід № 120554 С2, МПК H01Q 21/06, H01Q 13/08, Опубл. 26.12.2019, Бюл. № 24, заявка № а 2018 03104; від 26.03.2018.

4. The Order of Formation of Information Signals in IIoT /Alla Jammine, Serkov Alexandr, Bogdan Lazurenko, Nait-Abdesselam Farid // IJCSNS International Journal of Computer Science and Network Security, VOL.23 No.3, pp. 139-143. http://paper.ijcsns.org/07_book/202303/20230314.pdf

5. Дробик О. В., Лаптєв О. А., Пархоменко І. І., Богуславська О. В., Пепа Ю. В., Пономаренко В. В. Розпізнавання радіосигналів на основі апроксимації спектральної функції у базисі передатних функцій резонансних ланок другого порядку. Сучасний захист інформації. 2024. №2. С.13-23. https://doi.org/ 10.31673/2409-7292.2024.020002

6. Лаптєв О.А. Експериментально-статистичний метод обчислення кореляційної взаємозалежності параметрів розпізнавання засобів негласного отримання інформації. Сучасний захист інформації: науково-технічний журнал. К.: ДУТ, 2019. № 3(39)., С 23 – 29.

7. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

8. Мілевський С. В., Костяк М. Ю., Мілов О. В., Погасій С. С. Засоби моделювання поведінки агентів в інформаційно-комунікаційних системах Системи, навігації, управління та зв'язку. 6(58), 2019. – С. 63–70. Стаття фахове видання

9. NIST AI 100-1 Artificial Intelligence Risk Management Framework (AI RMF 1.0) This publication is available free of charge from: https://doi.org/10.6028/NIST.AI.100-1 January 2023

10. Толкачов М.Ю., Дженюк Н.В., Захаржевський А.Г., Погасій С.С., Глухов С.І. (2024) Метод захисту інформаційних ресурсів на основі семіотичної моделі кіберпростору. Сучасний захист інформації. № 1(57). С. 57–68. https://doi.org/10.31673/2409-7292.2024.010007,

11. Tolkachov, M., Dzheniuk, N., Yevseiev, S., Lysetskyi, Y., Shulha, V., Grod, I., Faraon, S., Ivanchenko, I., Pasko, I., & Balagura, D. (2024). Development of a method for protecting information resources in a corporate network by segmenting traffic. Eastern-European Journal of Enterprise Technologies, 5(9 (131), 63–78. https://doi.org/10.15587/1729-4061.2024.313158

12. Valentyn Sobchuk, Iryna Zelenska and Oleksandr Laptiev. Algorithm for solution of systems of singularly perturbed differential equations with a differential turning point. Bulletin of the Polish Academy of Sciences Technical Sciences, Vol.71, No 3, 2023, Article number: e145682. https://doi.org/ 10.24425/bpasts.2023.145682.

13. NIST. (2022) Security and privacy controls for federal information systems and organizations. (U.S. Department of Commerce, Washington, D.C.), NIST Special Publication 800-53, Rev 4., [Online Document], 2022. Available: http://dx.doi.org/10.6028/NIST.SP.800-53r4. [Accessed: March 27, 2022]

14. NIST. 2011a. NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. National Institute of Standards and Technology, September 2011. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

15. Барабаш О. В., Лаптєв О. А., Свинчук О. В., Соловйов Є. В., Бушков В. Г. Оцінка завадостійкості тракту виявлення радіосигналів. Сучасний захист інформації: науково-технічний журнал. К.: ДУТ, 2020. № 1, С. 18 – 24.

16. We Are Social, Hootsuite. Digital 2024: Global Overview Report. URL: https://wearesocial.com (дата звернення: 18.11.2024).

17.Cisco. Annual Internet Report (2018–2023). URL: https://www.cisco.com (дата звернення: 18.11.2024).

18. Sandvine. The Global Internet Phenomena Report 2024. URL: https://www.sandvine.com (дата звернення: 18.11.2024).

19. App Annie. State of Mobile 2024 Report. URL: https://www.data.ai (дата звернення: 18.11.2024).

20. Ofcom. Online Nation Report 2024. URL: https://www.ofcom.org.uk (дата звернення: 18.11.2024).

21. Barabash O., Laptiev O., Grushina O. The conceptual model of the intelligent network. Сучасний захист інформації, No4 (56), 2023, P. 1-9. https://doi.org/ 10.31673/2409-7292.2023.030202.

22. [ITU-T M.3010] Recommendation ITU-T M.3010 (2000), Principles for a telecommunications management network

23. NIST Special Publication 800-207. Zero Trust Architecture. (U.S. Department of Commerce). National Institute of Standards and Technology Special Publication 800-207 Natl. Inst. Stand. Technol. Spec. Publ. 800-207, 59 pages (August 2020) CODEN: NSPUE2. This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Надійшла 24.11.2024